REMARKS

The Office Action dated August 25, 2004 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Claims 1-8 and 19-21 are currently pending in the application and are respectfully submitted for consideration.

In the Office Action, claims 1, 2, 6, 19, 20, and 21 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dean (U.S. Patent No. 6,173,173) in view of Rudokas (U.S. Patent No. 6,185,416). The Office Action took the position that Dean discloses all of the elements of the claims, with the exception of detaching a registered terminal from a network. The Office Action then relies upon Rudokas to cure the acknowledged deficiency in Dean. This rejection is respectfully traversed for the reasons which follow.

Claim 1, upon which claims 2-8 are dependent recites a method for performing a detach of a terminal registered to a telecommunication network by associating an identification for the terminal, deriving a signature for the identification, and allocating a pair consisting of the identification and the signature to the terminal. The method includes the steps of sending a detach request including the identification and the identification signature from the registered terminal to the network and receiving the detach request at the network side. The method also includes the steps of comparing the received detach request with a record of registration data of the terminal kept at the

network side and detaching the terminal from the network, if the received detach request coincides with the record of registration data.

Claim 19 recites a terminal device adapted to the method according to claim 1. Claim 20 recites a network controlling device adapted to the method according to claim 1. Claim 21 recites a telecommunication system consisting of at least one terminal and at least one network controlling device controlling at least one radio transceiver device, adapted to carry out the method according to claim 1.

As a result of the claimed invention, a system and method for performing a secure detach procedure in a radio telecommunication network is provided. One advantage of the present invention is that a simple and useful method is provided for preventing a malicious user from interrupting a third party's calls by sending detach messages with random identities to mobile stations.

As will be discussed below, the cited prior art references of Dean and Rudokas fail to disclose or suggest all of the elements of the claims, and therefore fail to provide the advantages discussed above.

Dean discloses an enhanced kill call capability system where a plurality of vendor computers are linked with a mobile service center through a kill-call server. The vendor computers have means for detecting an invalid mobile call, preferably by monitoring RF fingerprints in the case of fraudulent calls by "clones" and by monitoring the remaining credit balance of metered, pre-paid calls. Col. 3, lines 17-32. The mobile service center includes an administrative call processing node for performing the actual call processing

and a mobile center for enabling a technician interface to terminate an invalid call. When the technician interface is made, the request is validated before any affirmative action is taken. Once validation is complete, a tear down request message is formatted and sent to the administrative call processing node. The administrative call processing node determines if the call is active and forwards the message to the appropriate call database node. Once the call database node has completed its task, the results are forwarded to the client. Col. 3, line 45-Col. 4, line 10.

Dean further discloses that the technician interface includes the mobile ID number of the call that is to be torn down and an identifier for a kill-call command. Col. 5, lines 5-15. When a client request that a call be torn down, the server validates a connection request with the client by obtaining the client's host name and IP address, and looking it up in a server table to verify that the client is authorized to perform call tear down. For security purposes a challenge is sent from the server to the client. The server uses the plain text password for the client as found in a flat file database along with the challenge to generate a signature for authentication. The client uses the challenge along with the shared secret password to create a signature and then sends the kill call request to the server with the client generated signature embedded in the request. The server compares the client generated signature with the server generated signature to verify that the client has authority to use the requested command. The kill call request is forwarded to the administrative call processing/data base node for actual tear down. Once the administrative call processing/data base node has completed its task, the kill call results

are sent back and reformatted with the information defined in the protocol specification and returned to the client. Col. 7, line 24 – Col. 8, line 6.

Rudokas discloses a method and apparatus for fraud control in cellular telephone systems. Call records are scanned to identify a fraudulent cellular phone based on its behavior. An identifier, such as an RF signature, representative of the fraudulent cellular phone is stored in fraud control equipment located at a cell site. A database of identifiers may comprise a positive validation database storing identifiers for all valid cellular phones used in the cellular telephone system. Alternatively, a negative validation database storing the identifiers for known fraudulent cellular phones may be used. A control channel editor intercepts a call origination request transmitted from a cellular phone to the cell site, and compares one or more characteristics of the cellular phone transmitting the call origination request to the database of identifiers. The control channel editor then prevents the completion of the phone call when the comparison indicates that the cellular phone is fraudulent. The call origination request can be prevented from completing by rerouting the call to a customer service number, interrupting the call origination request, transmitting a hang-up message to the phone, transmitting a hang-up message to the cell site, or transmitting a tear-down message to a switch.

Applicants respectfully submit that Dean and Rudokas, whether viewed alone or in combination, fail to disclose or suggest the elements of the present claims. Claim 1 recites, in part, performing a detach of a terminal registered to a telecommunication

network by sending a detach request including the identification and the identification signature from the registered terminal to the network. Dean, on the other hand, is simply directed to tearing down fraudulent calls in the mobile home market of the mobile telephone service subscriber (Dean, Col. 3, lines 1-9). Dean does not teach or suggest detaching a registered terminal from a network as recited in claim 1. Even though Dean may tear down a call, since there is no suggestion or discussion in Dean et al. of detaching a registered terminal from a network, the terminal initiating the fraudulent call in Dean may remain registered with and attached to the network. Therefore, according to the teaching of Dean, a new call can be initiated by the same terminal immediately after a previous call from that terminal has been "killed."

Claim 1 also recites sending a detach request including the identification and the identification signature from the registered terminal to the network. According to Dean, when a tear down request is received, the server (1) validates a connection request by obtaining the client's host name and IP address and looking up the host name and IP address in a server table to verify that the client is authorized to perform call tear down; (2) generates a signature created from a server generated challenge and the plain text password for the client; and (3) compares the server generated signature with the client generated signature received in the request from the client. There is no teaching in Dean of sending a detach request which includes both the identification and the identification signature from the registered terminal to the network, wherein the detach request is compared with a registration record and the terminal is detached if the received detach

request matches the registration record as recited in claim 1. The kill request of Dean includes only the client generated signature. As such, there is simply no teaching or suggestion in Dean of including the allocated pair with the identification and the identification signature in the kill call message.

Additionally, Rudokas fails to cure the deficiencies in Dean as discussed above. Rudokas discloses that calls detected as fraudulent are terminated in various ways, such as rerouting the call to a customer service number (Rudokas, Column 4, line 40 – Column 5, line 47). Rudokas, however, only discloses that the call is terminated. As a result, the terminal identified as the source of the fraudulent call remains registered. In other words, Rudokas does not disclose performing a de-registration of a registered fraudulent terminal. Thus, Rudokas also fails to disclose or suggest detaching a terminal from the network.

In addition, Rudokas only discloses that the terminal is identified by its mobile identity number (MIN) in combination with its electronic serial number (ESN) (Rudokas, Column 3, line 59 – Column 4, line 12). Applicants respectfully submit that neither the MIN nor the ESN represents an identification signature. Rudokas discloses that a terminal can be identified using an identification technique based on the comparison of radio frequency signatures for the cellular phones (Rudokas, Column 5, line 62 – Column 6, line 2) . However, the RF signature identification is only important because it provides a manner for independently identifying the fraudulent phone using the ESN or MIN. In other words, the RF signature of a terminal is unique to the terminal, but not derived

based on the terminal's identification represented by the MIN and ESN. As such, Rudokas also fails to disclose or suggest sending a detach request including the identification and the identification signature from the registered terminal to the network, as recited in claim 1.

For at least the reasons discussed above, Dean and Rudokas, whether viewed singly or in combination, fail to disclose or suggest all of the elements of claims 1, 19, 20, and 21, in addition to claims 2 and 6 which are dependent upon claim 1. Therefore, Applicants respectfully request that the rejection of these claims be withdrawn.

Claims 3-5 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dean in view of Rudokas and further in view of the well known prior art. The Office Action acknowledges that the combination of Dean and Rudokas fails to disclose or suggest that the predetermined state is a power off state. The Office Action then alleges, however, that the predetermined state is a power off state is well known in the art at the time of invention, and therefore it would have been obvious for a person of ordinary skill in the art to modify Dean with the teachings of the well known prior art since it is known that the phone is off if it is not in use or if there is no charge on the battery. The rejection is respectfully traversed for the following reasons.

Claims 3-5 are dependent upon claim 1, and therefore include all of the features recited in claim 1. The well known prior art cited in the Office Action does not cure the deficiencies of Dean and Rudokas as outlined above. Therefore, Applicant respectfully asserts that the rejection under 35 U.S.C. §103(a) should be withdrawn because Dean and

Rudokas in combination with the well known prior art does not teach or suggest each feature of claim 1 and hence, claims 3-5 which are dependent thereon.

Claims 7 and 8 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dean in view of Rudokas and further in view of Kuriki (U.S. Patent No. 5,765,105). The Office Action took the position that the combination of Dean and Rudokas discloses all of the elements of the claims, with the exception of temporary subscriber and international subscriber identity. The Office Action then relies upon Kuriki to cure this deficiency in Dean and Rudokas. The rejection is respectfully traversed for the following reasons.

Kuriki is directed to a GSM communication system which includes multiple mobile stations that share a single international mobile subscriber identity. When one of the mobile stations generates a call origination or call termination request, the mobile switching center provides the requested service only if the international mobile subscriber identity and the international mobile equipment identity attached to the mobile station is stored by the mobile switching center.

Kuriki also fails to cure the deficiencies in Dean and Rudokas. Kuriki fails to disclose or suggest sending a detach request including identification and identification signature from a registered terminal to a network, comparing the detached request with a record of registration data of the terminal kept at the network side, and detaching the terminal from the network, if the detached request coincides with the record of registration data as recited in independent claim 1. Therefore, Applicants respectfully

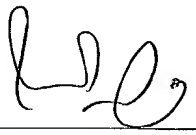
assert that the rejection under 35 U.S.C. §103(a) should be withdrawn because Dean, Rudokas, and Kuriki, whether taken singly or combined, fail to teach or suggest each feature of claim 1 and hence, claims 7 and 8 which are dependent upon claim 1.

Applicants respectfully submit that the cited prior art references fail to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-8 and 19-21 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf